Getting started

Symantec™ Client Security

About Symantec Client Security

Symantec Client Security provides scalable, cross-platform firewall, intrusion detection, and antivirus protection for workstations and antivirus protection for network servers. You can establish and enforce antivirus and firewall security policies; retrieve content updates, such virus definitions and intrusion detection signatures; control live viruses; and analyze logged events.

Symantec Client Security provides a variety of management tools. You can use a centralized management console, the Symantec System Center, running on an administrator computer to manage security on your network-connected computers and remotely deploy Symantec Client Security software. Additional tools allow you to set up internal distribution of content updates and automate responses to new or unrecognized viruses.

Computers that are not connected to your network can also be protected with Symantec Client Security. Content license files must be distributed to each computer.

Where to find information

Sources of information on using Symantec Client Security include the following:

- Readme file: Contains late-breaking information about installing and using Symantec Client Security
- Symantec Client Security *Installation Guide*: Provides the information that you need to plan and execute the installation of Symantec Client Security on your network
- Symantec Client Security *Administrator's Guide*: Provides the information that you need to manage Symantec Client Security using the Symantec System Center
- Symantec Client Security *Reference Guide*: Contains technical product information, including information on tools that are on the Symantec Client Security CD
- Symantec Client Security *Client Guide*: Provides the information that you need to use Symantec Client Security on a client computer

- *LiveUpdate Administrator's Guide*: Provides the information that you need to configure and manage the LiveUpdate Administration Utility
- Online Help: Contains all of the content found in the above guides and more

All of the documentation is available in the Docs folder on the Symantec Client Security CD. Updates to the documentation are available from the Symantec Technical Support and Platinum Support Web sites.

Additional information is available from the Symantec Web sites that are listed in the following table.

Table 1-1

Types of information	Web address
Public Knowledge Base Releases and updates Manuals and documentation Contact options	http://www.symantec.com/techsupp/enterprise/
Virus information and updates	http://securityresponse.symantec.com
Product news and updates	http://enterprisesecurity.symantec.com
Platinum support Web access	https://www-secure.symantec.com/platinum/

How to get started

This card describes the main methods for installing Symantec Client Security and provides the information that you need to run the product. For a description of all of the methods that you can use to install Symantec Client Security, including Windows Installer (.msi) technology, the Web Installer, third-party tools, and logon scripts, see the Symantec Client Security *Installation Guide*.

If you are upgrading from an earlier version of Symantec Client Security, see "Migrating to the current version of Symantec Client Security" in the Symantec Client Security *Installation Guide*.

To use this card to get started, do the following:

- Read about the Symantec Client Security components and determine the components that you want to install.
- Review the system requirements for the selected components.
- Review all preinstallation information and perform any required tasks.
- Select an implementation strategy as follows:
  - If you plan to use the Symantec System Center to manage Symantec Client Security and to deploy installations to managed computers, start with "Installing Symantec Client Security from the Symantec System Center" on page 5.
    If you plan to use the administration tools, continue with "Installing administration tools" on page 8.
  - If you will not use the Symantec System Center for installation rollout, start with "Installing Symantec Client Security locally from the CD" on page 9.
- After completing the installation, review the post-installation tasks.

Symantec Client Security components

Symantec Client Security lets you install only the components that you need to implement security at your site. Although you can install and manage the Symantec Client Security server and client programs without the Symantec System Center, a centrally managed implementation works best for most businesses.

The Symantec System Center is required if you want to manage Symantec Client Security servers and clients (including legacy antivirus clients) from a central console.

The following management components are installed by default when you install the Symantec System Center:

- Alert Management System^2 (AMS^2) console: Required if you want to use the enhanced alerting that is provided by AMS^2.
- Symantec AntiVirus snap-in: Required if you want to centrally manage antivirus protection.
- Symantec Client Firewall snap-in: Required for firewall client administration.
- AV Server Rollout tool: Required to push the antivirus server installation to remote computers. This tool is available on the Symantec Client Security CD.
- NT Client Install tool: Required to push the Symantec Client Security antivirus client installation to remote computers running supported Microsoft Windows operating systems. This tool is available on the Symantec Client Security CD.

- Symantec Client Security server: Required to manage networked computers running the Symantec Client Security client program. It also provides antivirus protection to the computers on which it runs. The server program lets you push antivirus and firewall security policies and content updates to managed clients. To protect a network server that does not manage Symantec Client Security clients, install the Symantec Client Security client program.
- Symantec Client Security client: Required for antivirus, firewall, and intrusion protection for networked and non-networked computers.
- Symantec Central Quarantine: Required if you want automated responses to heuristically detected new or unrecognized viruses. Central Quarantine works with Symantec Security Response to automatically repair infected files submitted from Symantec Client Security clients and servers.
- Symantec Client Firewall Administrator: Required if you want to create and modify firewall rules and intrusion detection signatures.
- LiveUpdate Administration Utility: Required if you want to set up an internal LiveUpdate server as a single download point for virus definitions and updates to Symantec products.

System requirements

This section includes system requirements for the main Symantec Client Security components. For system requirements for other components, see the Symantec Client Security *Installation Guide*.

Symantec System Center and snap-in requirements

The Symantec System Center requires the following:

- Windows NT 4.0 Workstation/Server with Service Pack 6a; Windows 2000 Professional/Server/ Advanced Server; Windows XP Professional; Windows Server 2003 Web/Standard/Enterprise/Datacenter
- 32 MB RAM
- 36 MB disk space (plus additional disk space for the snap-ins, which are listed separately)
- Internet Explorer 5.5 with Service Pack 2
- Microsoft Management Console version 1.2
  If MMC is not already installed, you will need 3 MB free disk space (10 MB during installation).

Note: If Microsoft Management Console version 1.2 is not on the computer to which you are installing, the installation program will install it.

The following snap-ins and installation tools have disk space requirements in addition to the Symantec System Center requirements:

- Symantec AntiVirus snap-in: 6 MB disk space
- Symantec Client Firewall snap-in: 1 MB disk space
- Quarantine Console snap-in: 35 MB disk space
- Alert Management System^2 snap-in: 24 MB disk space
- AV Server Rollout tool: 130 MB disk space
- NT Client Install tool: 2 MB disk space

Symantec Client Firewall Administrator requirements

The Symantec Client Firewall Administrator has the following requirements:

- Windows NT 4.0 Workstation/Server with Service Pack 6a; Windows 2000 Professional/Server/ Advanced Server; Windows XP Professional; Windows Server 2003 Web/Standard/Enterprise/Datacenter
- 64 MB RAM
- 80 MB disk space

Symantec Client Security server installation requirements

Symantec Client Security server runs under several operating systems, each with unique installation requirements.

You should assign a static IP address to Symantec Client Security servers. If a client is unavailable when its parent server's address changes, it will not be able to locate the parent server when it attempts to check in.

Microsoft Windows operating systems

Symantec Client Security server has the following Windows requirements:

- Windows NT 4.0 Workstation/Server/Terminal Server with Service Pack 6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional; Windows Server 2003 Web/Standard/ Enterprise/Datacenter
- 64 MB RAM
- 111 MB disk space

- 15 MB disk space for AMS^2 server files (if you choose to install the AMS^2 server)
- Internet Explorer 4.01 or later
- Static IP address (recommended)

Note: Symantec Client Security does not support scanning for Macintosh viruses on Windows servers with Macintosh volumes.

Novell NetWare operating systems

You should run the Novell Client for NetWare on the computer from which Symantec Client Security will be rolled out to NetWare servers.

Symantec Client Security server has the following NetWare requirements:

- NetWare 5.1 with Support Pack 3 or higher; NetWare 6.0 with Support Pack 1 or higher; NetWare 6.5
- 15 MB RAM (above the standard NetWare RAM requirements) for Symantec AntiVirus NLMs
- 116 MB disk space (70 MB disk space for antivirus server files and 46 MB disk space for the antivirus client disk image)

Note: Symantec Client Security is not supported on NetWare servers that are running SFT III.

Quarantine Server requirements

Quarantine Servers have the following requirements:

- Windows NT 4.0 Workstation/Server with Service Pack 6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional; Windows Server 2003 Web/Standard/Enterprise/Datacenter
- 64 MB RAM
- 40 MB disk space for Quarantine Server
- 500 MB to 4 GB disk space recommended for quarantined items
- Internet Explorer 5.5 with Service Pack 2
- Minimum swap file size of 250 MB

Note: If you are running Windows Me/XP, system disk space usage is increased if the System Restore functionality is enabled. For information on System Restore, see the Microsoft documentation.

Symantec Client Security client installation requirements

Requirements vary based on the type of protection installed to the computer. Disk space requirements are based on the installation of all features.

Symantec Client Security client (antivirus and firewall protection) for 32-bit computers

Symantec Client Security clients have the following requirements:

- Windows 98/98 SE/Me; Windows 2000 Professional; Windows XP Home/Professional

  Note: Windows NT 4.0 Workstation is supported only for Symantec Client Security antivirus clients installed from the Symantec System Center, which does not install firewall protection.

- 128 MB RAM minimum
- 80 MB disk space
- Internet Explorer 5.01 Service Pack 2 or later

Symantec Client Security antivirus client for 32-bit computers

Symantec Client Security antivirus clients for 32-bit computers have the following requirements:

- Windows 98/98 SE/Me; Windows NT 4.0 Workstation/Server/Terminal Server with Service Pack 6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Home/Professional/Tablet PC (for Windows XP Tablet PC, antivirus client only); Windows Server 2003 Web/Standard/Enterprise/Datacenter
- 32 MB RAM minimum
- 55 MB disk space
- Root Certificate Update (Windows 98/98 SE)

Terminal Server clients connecting to a computer with antivirus protection have the following additional requirements:

- Microsoft Terminal Server RDP (Remote Desktop Protocol) client
- Citrix Metaframe (ICA) client 1.8 or later

Symantec Client Security antivirus client for 64-bit computers

Symantec Client Security antivirus clients for 64-bit computers have the following requirements:

- Windows XP 64-bit Edition Version 2003; Windows Server 2003 Enterprise/Datacenter 64-bit
- 32 MB RAM minimum
- 70 MB disk space
- Internet Explorer 4.01 or later
- Itanium 2 processor

Before you install

Before you begin any installation procedure, you need to consider several factors.

Windows Installer (.msi) considerations

Symantec Client Security uses Windows Installer technology for all client and server installations. You can use the standard Microsoft Windows Installer options with the Symantec Client Security settings to configure the installation of Symantec Client Security-specific features.

In addition to the standard installation methods, you can deploy client or server installations using .msi-supported third-party tools such Active Directory and Tivoli.

See the Symantec Client Security *Installation Guide*.

Server considerations

The following are server considerations:

- When you are installing to NetWare, log on to all of the NetWare servers before you start the installation. To install to NetWare Directory Services (NDS) or bindery, you need administrator or supervisor rights.
- When you install to NDS, the computer that is performing the installation must use the Novell Client for NetWare. If you encounter problems installing to a bindery server with the Microsoft Client for NetWare, install the Novell Client for NetWare and try again.
- Symantec recommends that you run the Novell Client for NetWare on the computer from which Symantec Client Security server will be rolled out to NetWare servers.

Client considerations

The Symantec Client Security client installation program triggers the uninstallation of the following firewall products:

- Symantec Client Security, all versions
- Symantec Client Firewall 5.0/5.1
- Norton Personal Firewall 2003
- Symantec Desktop Firewall 2003

You must manually uninstall all other versions before installing Symantec Client Security firewall client, including Norton Personal Firewall version 2004.

Quit all other Windows programs before installing Symantec Client Security firewall client. Other active programs may interfere with the installation.

Note: Installing Symantec Client Security firewall client without Symantec Client Security antivirus client is not supported.

Disabling the Windows XP firewall

Windows XP includes a firewall that can interfere with Symantec Client Security firewall client protection features. You must disable the Windows XP firewall before installing Symantec Client Security firewall client.

To disable the Windows XP firewall

1. On the Windows XP taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Network Connections**.
3. In the Network Connections window, right-click the active connection, and then click **Properties**.
4. On the Advanced tab, in the Internet Connection Firewall section, uncheck **Protect my computer and network by limiting or preventing access to this computer from the Internet**.
5. To close the settings window, click **OK**.

Installing Symantec Client Security from the Symantec System Center

You can install the Symantec System Center and use the management console to deploy the installation of managed servers and clients.

The installation of the Symantec System Center includes installation of all of its management components by default. You can deselect any component that you do not want to install.

If you do not want to use the Symantec System Center, continue with "Installing Symantec Client Security locally from the CD" on page 9.

Installing the Symantec System Center

Install the Symantec System Center to the computer from which you want to manage antivirus and firewall protection.

To install the Symantec System Center

1. Insert the Symantec Client Security CD into the CD-ROM drive.
2. In the Symantec Client Security panel, click **Install Administrator Tools** > **Install Symantec System Center**.
3. Follow the on-screen instructions.

Installing the server program

Install the server program to any computer that will manage clients. You must designate at least one server as a primary server.

To start the server installation

1. In the Symantec System Center, in the left pane, do one of the following:
   - Click **System Hierarchy**.
   - Under System Hierarchy, select any object.
2. On the Tools menu, click **AV Server Rollout**.
   AV Server Rollout is available only if you selected the Server Rollout component when you installed the Symantec System Center. This component is selected for installation by default.
3. Continue the installation.
   See "To run the server setup program" on page 6.

To run the server setup program

1. In the welcome panel, do one of the following:
   - To install the server to computers that have never had Symantec Client Security installed, click **Install**, and then click **Next**.
   - To install the server to computers that have had Symantec Client Security previously installed, click **Update**, and then click **Next**.
2. In the License Agreement panel, click **I agree**, and then click **Next**.
3. In the Select Items panel, ensure that Server program is checked.
   If you plan to use Alert Management System^2 (AMS^2), ensure that it is checked.
4. Click **Next**.
5. To continue the installation, do one of the following:
   - Manually select Windows computers.
     See "To manually select Windows computers" on page 6.
   - Import a list of Windows NT/2000/XP/2003 computers.
     If you are installing in a non-WINS environment, you must select computers by importing a text file that contains the IP addresses of the computers to which you want to install. You can use the same import method in a WINS environment. This method is not intended for use with NetWare.
     For instructions on how to import a list of Windows NT-based computers, see the Symantec Client Security *Installation Guide*.

To manually select Windows computers

1. In the Select Computers panel, under Network, expand **Microsoft windows network**.
2. Select a server on which to install, and then click **Add**.
3. Repeat step 2 until all of the servers to which you are installing are added under Destination computers.
4. Select any NetWare computers to which you want to install.
   See "To manually select Novell NetWare computers" on page 6.
5. Continue the installation.
   See "To complete the server installation" on page 7.

To manually select Novell NetWare computers

1. In the Select Computers panel, under Available Computers, double-click **NetWare Services**.
2. Do one of the following:
   - To install to a bindery server, double-click **NetWare Servers**, and then select a server (indicated by a server icon).
   - To install to NDS, double-click **Novell Directory Services**, and then select the SYS volume object in which you want to install Symantec Client Security.
     To locate a SYS volume object, double-click the tree object and continue expanding the objects until you reach the organizational unit that contains the SYS volume object.
3. Click **Add**.
4. If you are installing to NDS, you are prompted to type a container, user name, and password.
   If you type an incorrect user name or password, the installation continues normally. However, when you

attempt to start Symantec Client Security on the NetWare server, you receive an authentication error and are prompted for the correct user name and password.

5 Repeat steps 1 through 4 until the volumes for all of the servers that you are installing to are added under AntiVirus Servers.

6 Select any Windows computers to which to install.
See "To manually select Windows computers" on page 6.

7 Continue the installation.
See "To complete the server installation" on page 7.

To complete the server installation

1 In the Select Computers panel, click **Finish**.

2 In the Server Summary panel, do one of the following:

- To accept the default Symantec Client Security installation path, click **Next**.
- To change the path, select a computer, and then click **Change Destination**. In the Change Destination dialog box, select a destination, click **OK**, and then click **Next**.
  If you are installing to a NetWare server, the new folder name is limited to 8 characters.

3 In the Select Symantec AntiVirus Server Group panel, do one of the following:

- Under Symantec AntiVirus Server Group, type a name for a new server group, and then click **Next**. You will be prompted to confirm the creation of the new server group and to specify a password for the server group.
- In the list, select an existing server group to join, click **Next**, and then type the server group password when you are prompted.

4 Select one of the following:

- Automatic startup: On a NetWare server, you must manually load Vpstart.nlm after you install Symantec Client Security server, but Vpstart.nlm will load automatically thereafter. (You must either create or join a server group during the installation process before this takes effect.)
  On a Windows NT-based computer, Symantec Client Security services (and AMS^2 services, if you installed AMS^2) start automatically every time that the computer restarts.
- Manual startup: On a NetWare server, you must manually load Vpstart.nlm after you install Symantec Client Security server and every time that the server restarts. Selecting this option will have no effect on Windows NT-based computers.

5 Click **Next**.

6 In the Using the Symantec System Center Program panel, click **Next**.

7 In the Setup Summary panel, read the message that reminds you that you will need your password to unlock the server group in the Symantec System Center, and then click **Finish**.

8 In the Setup Progress panel, view the status of the server installations.

9 Finish the installation.
When Symantec Client Security server is installed to all of the computers that you specified, you can check to see if any errors were reported.
See "To check for errors" on page 7.

To check for errors

1 In the Setup Progress panel, select a server, and then click **View Errors**.

2 When you are done, click **Close.**

Note: When installing to a Windows NT computer, you must restart the computer after installation completes.

If you've installed to any NetWare computers, you need to load the appropriate NLMs.

See the Symantec Client Security *Installation Guide*.

Installing the client program

Install the client program to all clients that you want to be managed from the Symantec System Center.

To start the client installation

1 In the Symantec System Center, in the left pane, do one of the following:

- Click **System Hierarchy**.
- Under System Hierarchy, select any object.

2 On the Tools menu, click **NT Client Install**.
NT Client Install is available only if you selected the NT Client Install tool when you installed the Symantec System Center. This component is selected for installation by default.

3 Continue the installation.
See "To run the client setup program" on page 8.

To run the client setup program

1. In the welcome panel, click **Next**.
2. In the Select Install Source Location panel, select the location from which you are deploying the client installation files.
3. After you have selected the location, click **Next**.
4. In the Select Computers panel, under AntiVirus Servers, select a computer to act as a parent server.
5. Under Available Computers, expand **Microsoft windows network**, and then select a computer.
6. Click **Add**.
7. Repeat steps 5 and 6 until all of the clients that you want to manage are added.
   You can reinstall to computers that are already running Symantec Client Security. You can also import a text file to add Windows NT-based clients.
8. Do one of the following:
   - If you created a text file that contains IP addresses to import computers that are in non-WINS environments, continue to step 9.
   - If you did not create a text file that contains IP addresses to import computers in non-WINS environments, continue to step 11.
9. To import the list of computers, click **Import**.
10. Locate and double-click the text file that contains the computer names.
    A summary list of computers to be added under Available Computers appears.
    During the authentication process, you may need to provide a user name and password for computers that require authentication.
11. In the Selection Summary dialog box, click **OK**.
    During the authentication process, Setup checks for error conditions. You are prompted to view this information interactively on an individual computer basis or to write the information to a log file for later viewing.
12. When you are prompted to view the error information, select one of the following:
    - Yes: Display the information on an individual computer basis.
    - No: Write it to a log file.
      If you create a log file, it is located under C:\Winnt\Savcecln.txt.
13. In the Select Computers panel, click **Finish**.
14. In the Status of Remote Client Installations window, click **Done**.

Installing administration tools

Install the administration tools that you want to use to manage security at your site.

Installing Central Quarantine

The Quarantine Console snap-in must be installed to a computer running the Symantec System Center. Install the Quarantine Server to a computer that you want to use to store infected files.

To install the Quarantine Console snap-in

1. On the computer on which the Symantec System Center is installed, insert the Symantec Client Security CD into the CD-ROM drive.
   If your computer is not set to automatically run a CD, you must manually run Setup.exe.
2. In the Symantec Client Security panel, click **Install Administrator Tools** > **Install Quarantine Console**.
3. Follow the on-screen instructions.

To install the Quarantine Server

1. On the computer on which you want to install the Quarantine Server, insert the Symantec Client Security CD into the CD-ROM drive.
2. In the Symantec Client Security panel, click **Install Administrator Tools** > **Install Central Quarantine Server**.
3. Follow the on-screen instructions.

For more information, see the *Symantec Central Quarantine Administrator's Guide* PDF on the Symantec Client Security CD.

Installing Symantec Client Firewall Administrator

Symantec Client Firewall Administrator is installed directly from the CD.

To install Symantec Client Firewall Administrator

1. Insert the Symantec Client Security CD into the CD-ROM drive.
2. In the Symantec Client Security panel, click **Install Administrator Tools** > **Install Symantec Client Firewall Administrator**.
3. Follow the on-screen instructions.

Installing the LiveUpdate Administration Utility

Install the LiveUpdate Administration Utility on a Windows NT computer that is running the antivirus server program, and then configure it.

To install the LiveUpdate Administration Utility

1. Insert the Symantec Client Security CD into the CD-ROM drive.
2. In the Symantec Client Security panel, click **Install Administrator Tools** > **Install LiveUpdate Administrator**.
3. Follow the on-screen instructions.

For more information, see the *LiveUpdate Administrator's Guide* PDF on the Symantec Client Security CD.

Installing Symantec Client Security locally from the CD

You can install Symantec Client Security directly from the Symantec Client Security CD. To determine whether you need to install the server program or client program, do the following:

- If you want a server to manage virus definitions updates, policy settings, and configurations for other networked Symantec Client Security servers and clients, install the server program.
- If you want to protect computers that do not manage Symantec Client Security clients, or if you want to protect either managed or unmanaged client computers, install the client program.
  When you install the client program, you specify whether the client is managed or unmanaged. Managed clients must specify the name of the parent server.

Installing the server locally

The server program allows you to manage other computers running Symantec Client Security.

To install the server locally

1. From the Symantec Client Security CD, in the \SAV folder, run Setup.exe.
2. In the welcome panel, click **Next**.
3. Follow the on-screen instructions.
   During the installation, you will be offered the following choices:
   - Client Server Options panel: Click **Server**.
   - Setup Type panel: Click **Complete** to install all of the components that are included with the default installation or **Custom** to select components.
   - Select Server Group panel: Type the name of an existing server group and the password for that group or type the name of a new server group and create a password.
   - Install Options panel: Check **Auto-Protect** if you want to enable Auto-Protect. Check **LiveUpdate** if you want LiveUpdate to run at the end of the installation. If you chose to run LiveUpdate after installation, follow the instructions in the LiveUpdate Wizard.

Installing the client locally

The client program protects the computers on which it runs.

To install the client locally

1. From the Symantec Client Security CD, do one of the following:
   - For installation on a 32-bit computer, in the root of the CD, run Setup.exe.
   - For installation on a 64-bit computer, run Setup.exe from the \SAVWIN64 folder. Continue with step 3.

   Warning: If the 32-bit version of Setup.exe is run on a 64-bit computer, the installation may fail without notification. For 64-bit installations, users must run Setup.exe from the \SAVWIN64 folder in the root of the CD.
2. In the Symantec Client Security panel, click **Install** Symantec Client Security > **Install** Symantec Client Security
3. In the welcome panel, click **Next**.
4. Follow the on-screen instructions.
   During the installation, you will be offered the following choices:
   - Setup Type panel: Click **Complete** to install all of the components that are included with the default installation or **Custom** to select components.
   - Network Setup Type panel: Click **Managed** to have the client managed by a parent server or **Unmanaged** to run without a parent server. If you select Managed, you must know the name of

the Symantec Client Security server to which the client will connect.

- Install Options panel: Check **Auto-Protect** if you want to enable Auto-Protect. Check **LiveUpdate** if you want LiveUpdate to run at the end of the installation. If you chose to run LiveUpdate after installation, follow the instructions in the LiveUpdate Wizard.

Post-installation tasks

After installation, you should do the following:

- Create a primary server for each server group.
- Perform a content update using the method of your choice, such as LiveUpdate.
- Set up and distribute your security policies.
- Run a virus scan on all protected computers.

For information on how to perform management tasks, see the Symantec Client Security *Administrator's Guide*.

What's new in this release

Symantec Client Security includes new and improved features. The following table lists and describes what's new in this release.

Feature	Description
Windows Installer (.msi) client and server installations	Lets you install Symantec Client Security clients and servers using Windows Installer technology to support .msi-based installation and deployment.
Deployment of installations without granting administrator rights on the target computer	Lets you install Symantec Client Security from the Microsoft Management Console (MMC) using Elevated Privileges, rather than granting administrative privileges to the user on the target computer.
Auto-Protect	Replaces and scans faster than Realtime File Protection. Auto-Protect can be loaded on system startup, and then unloaded on system shutdown to help protect against viruses, such as Fun Love.
In-memory threat scanning	Lets you scan running processes to identify and handle threats that are loaded into memory.
Threat Tracer	Lets you identify, by IP address and NetBIOS name, the source of network share-based virus infections on computers that are running Windows NT-based operating systems.
Forced LiveUpdate for Symantec Client Security clients	Provides a way to update virus definitions files when clients on which LiveUpdate is installed are using outdated files.
Expanded threat detection	Scans for new threats in the following categories: Spyware, Adware, Dialers, Joke Programs, Remote Access programs, Hack Tools, and Trackware. Other threats that do not meet these category requirements are included in the Security Risks category.
Moving clients between servers	Lets you move clients from one parent server to another using a drag-and-drop operation.
Symantec VPN Sentry	Prevents users with nonsecure computers from connecting to a corporate network through a VPN connection and ensures that a computer that is attempting to connect is compliant with the corporate security policy.
Log forwarding	Lets you select the events that clients forward to their parent servers and that secondary servers forward to primary servers.
POP3 and SMTP Internet email scanning	Lets you configure Symantec Client Security clients to scan email body text and attachments that are transported using the POP3 or SMTP protocols. The ports scanned for POP3 and SMTP traffic are configurable.
Outbound email heuristics scanning	Lets you enable outbound email heuristics scanning, which uses Bloodhound Virus Detection to identify potential threats contained in outgoing messages. This feature helps prevent the spread of threats such as worms that use email clients to replicate and distribute themselves across a network.
Alert Assistant	Helps you understand firewall alerts and potential security issues.

Feature	Description
Log Viewer	Improved viewer helps you see all of the actions that Symantec Client Security firewall client takes to protect your computer.
Privacy Control	Enhanced version blocks private information in Web browsers, email messages, and instant messages.
Location Awareness	Lets you implement specific sets of firewall rules and zones based on the network access point used to connect to the Internet.
Secure Port	Secures the ports defined in Trojan horse rules so completely that traffic destined for these ports, both inbound and outbound, never triggers firewall rulebase inspection.
Settings Manager	Lets you export and import firewall policy files to provide backup and restore functionality.
Ad Blocking	Enhanced version lets you tailor firewall settings for specific Web sites and HTML strings.